
OLR Bill Analysis

sSB 397 (as amended by Senate "A" and "B")*

AN ACT CONCERNING DEMOCRACY AND GOVERNMENT ACCOUNTABILITY.

TABLE OF CONTENTS:

SUMMARY

§§ 1 & 2 — ACTIONS FOR CIVIL RIGHTS VIOLATIONS

Creates an individual cause of action, including against a federal or state officer or employee, for alleged civil rights violations; expands the attorney general's authority to bring actions based on alleged civil rights violations

§§ 3-5 — INSPECTOR GENERAL USE OF FORCE INVESTIGATIONS

Changes when there must be an investigation of a peace officer's use of physical force on someone that results in the person's death or the death of a person in custody by (1) limiting the investigations to deaths that occur in physical custody and (2) requiring an investigation when the officer is any federal law enforcement officer; requires investigators to have unrestricted access to the scene and to collect evidence; requires the inspector general's post-investigation report to recommend actions for the law enforcement agency involved and allows the inspector general to issue a report after a DOC custody death investigation

§ 6 — PROHIBITED FACIAL COVERINGS

Prohibits, subject to several exceptions, peace officers from wearing a facial covering or personal disguise when interacting with the public and performing law enforcement duties; makes a violation a class D misdemeanor

§ 6 — BADGE AND NAME TAG IDENTIFICATION

Generally, requires peace officers to be clearly identified by their badge and name tag when making a planned, authorized arrest or interacting with the public in an official capacity; makes an intentional violation a class D misdemeanor

§§ 7 & 8 — TAKING INTO CUSTODY IN STATE OR MUNICIPAL FACILITIES OR PROTECTED AREAS

Prohibits peace officers from taking someone into custody on the basis of a civil offense in a state or municipal facility or certain other locations such as schools, hospitals, and houses of worship ("protected areas") without a judicial warrant for the person; applies the definition of "civil offense" to the existing restrictions on taking people into custody on courthouse grounds

[§ 9 — POST CERTIFICATION OF POLICE OFFICERS](#)

Prohibits POST from waiving the basic training program requirements to be certified as a police officer for peace officers unless they give evidence of satisfactorily completing a substantially equivalent training or education program with at least 480 training hours

[§ 10 — OFFICER INTERFERENCE WITH PHOTO OR VIDEO TAKING](#)

Makes federal law enforcement agencies liable when their officers interfere with someone taking a photo, digital still, or video image of them or another officer performing their duties; makes an immunity defense unavailable in a civil liability action for an intentional tort committed while interfering with the taking of the photo, digital still, or video image

[§ 11 — PROSECUTORIAL IMMUNITY FOR FEDERAL ACTIONS](#)

Limits the circumstances under which a federal officer, employee, or agent has immunity when prosecuted for an offense based on an action taken under color of law

[§ 12 — POLICE OFFICER HIRING PROHIBITION](#)

Extends to all peace officers the current prohibition on hiring police officers who (1) were dismissed for malfeasance or serious misconduct or (2) resigned or retired during an investigation for this conduct

[§§ 13-15 — AUTOMATED LICENSE PLATE READER SYSTEMS](#)

Sets various conditions and restrictions on how law enforcement agencies and other public agencies may use ALPR systems or associated data, including limits on (1) when they can use these systems or data or share the data and (2) how long they can keep the data; sets related requirements and restrictions for private vendors contracting with public agencies for these purposes; allows the attorney general (as to vendors) or private parties to seek related court relief and POST to discipline law enforcement officers for certain malicious conduct; requires POST to adopt a model ALPR usage policy and DESPP to adopt related regulations for implementation by law enforcement agencies; requires POST, in consultation with UConn’s Institute for Municipal and Regional Policy, to develop a standardized form for reporting ALPR system usage and sets related reporting requirements

[BACKGROUND — RELATED BILLS](#)

SUMMARY

This bill makes various changes to laws related to civil rights and law enforcement activity, as shown in the section-by-section analysis below. It also makes technical and conforming changes.

*Senate Amendment “A” (1) limits the inspector general’s use of force death investigations to those that happened in physical custody only; (2) allows the inspector general to issue a report about a death in the Department of Correction’s (DOC) physical custody; (3) makes weather and traffic safety concerns conditions under which peace officers are exempt from the bill’s requirement to have their name tag and badge on their outermost clothing; (4) removes the underlying bill’s general ban

on armed military forces from other states, territories, or districts coming to Connecticut for military duty; (5) delays, from upon passage to October 2026, the effective date of the restrictions on taking someone into custody for a civil offense, defines “civil offense,” and narrows the scope of the locations subject to the protections; (6) prohibits the Police Officer Standards and Training Council (POST) from waiving basic training requirements for peace officers unless they satisfactorily complete a substantially equivalent training or education program with at least 480 training hours, instead of generally codifying POST’s comparative certification regulations; (7) adds the automated license plate reader (ALPR) provisions; and (8) makes various minor, technical, and conforming changes.

*Senate Amendment “B” (1) extends the bill’s ALPR data retention period for criminal investigations to the end of the defendant’s prison term, when applicable, and (2) removes a provision that would have prohibited private vendors from holding the contracting agency’s ALPR data out of state.

EFFECTIVE DATE: Upon passage, except the provision restricting taking someone into custody for a civil offense in certain locations is effective October 1, 2026.

§§ 1 & 2 — ACTIONS FOR CIVIL RIGHTS VIOLATIONS

Creates an individual cause of action, including against a federal or state officer or employee, for alleged civil rights violations; expands the attorney general’s authority to bring actions based on alleged civil rights violations

Individual Cause of Action

Scope of Action. The bill creates a cause of action (in court or another proper proceeding) against an individual, including a federal or state officer or employee, that deprives or causes a Connecticut citizen or someone within the state’s jurisdiction to be deprived of a right, privilege, or immunity protected by the U.S. Constitution. This can occur by taking actions under color of United States or Connecticut statute, regulation, ordinance, custom, or usage.

The bill explicitly states that it is the legislature’s intent that courts, when considering this action, must be guided by other courts’

interpretations of the law that allows individuals to sue state or local government officials for federal constitutional rights violations (42 U.S.C. § 1983).

Defenses. The bill (1) allows the defendant in a civil action to raise any applicable immunities, including sovereign immunity, given by state or federal law and (2) protects federal officers and employees from civil liability to the same extent the law does for equivalent state officers or employees (such as personal immunity from civil liability for damage caused when discharging duties or within the scope of employment unless an action was wanton, reckless, or malicious).

Damages. The bill allows the court to award damages, including nominal, actual, compensatory, or punitive damages; injunctive relief; or other equitable relief. It specifies that the purpose of the damage award is to protect the peaceable exercise or enjoyment of rights given by the U.S. Constitution.

The bill requires the court to award the plaintiff reasonable attorney's fees and expenses, unless it determines that there are special circumstances that would make doing so unjust.

Attorney General Authority to Bring an Action

Practice, Pattern of Conduct, Policy. Existing law authorizes the state attorney general to investigate, intervene in, and bring civil or administrative actions on behalf of the state when there is a practice or pattern of conduct that:

1. deprives persons of any rights, privileges, or immunities protected by the U.S. or Connecticut constitutions or laws or
2. interferes by threats, intimidation, or coercion, with another persons' exercise or enjoyment of any rights, privileges, or immunities protected by the U.S. or Connecticut constitutions or laws, or any attempt to do so.

The bill broadens the attorney general's authority to take these actions on behalf of the state by also allowing him to do so when any

one has established a policy that deprives or interferes with another person's civil rights in the ways described above.

Actions Under Color of Law or Custom. The bill also expands the attorney general's authority to investigate, intervene in, or bring a civil or administrative action by allowing him to do so when someone acts under the appearance of authority from a federal or state statute, regulation, ordinance, custom, or usage ("color of law") in a way that:

1. deprives another person of any rights, privileges, or immunities protected by the U.S. or Connecticut constitutions or
2. interferes by physical obstruction, threats, intimidation, or coercion, with another person's exercise or enjoyment of any rights, privileges, or immunities protected by the U.S. or Connecticut constitutions.

Court Process. For the bill's new actions based on acts done under the appearance of authority, the attorney general may bring the action in the Superior Court for the judicial district where the violation or alleged violation occurred. The bill requires the court to have a hearing on the complaint within five days after its filing, and the attorney general to notify the interested parties of its time and location. If all parties agree, the court may reschedule the hearing. The court may order declaratory relief (a statement of rights) or a temporary injunction once the complaint is filed. After the hearing, it may order, amend, or continue the relief or injunction.

§§ 3-5 — INSPECTOR GENERAL USE OF FORCE INVESTIGATIONS

Changes when there must be an investigation of a peace officer's use of physical force on someone that results in the person's death or the death of a person in custody by (1) limiting the investigations to deaths that occur in physical custody and (2) requiring an investigation when the officer is any federal law enforcement officer; requires investigators to have unrestricted access to the scene and to collect evidence; requires the inspector general's post-investigation report to recommend actions for the law enforcement agency involved and allows the inspector general to issue a report after a DOC custody death investigation

By law, the Division of Criminal Justice (DCJ) must investigate whenever a peace officer, while performing his or her duties, uses physical force on someone that causes that person's death or uses

deadly force (a type of physical force) on another person. The inspector general is responsible for determining if the use of force was justifiable.

Similarly, current law requires the inspector general to investigate any death that happened while the person was in the custody of a peace officer, law enforcement agency, or DOC to determine if physical force was used on the person and if it was justifiable. The bill limits these investigations to circumstances involving the death of someone in physical custody, rather than any custody (such as the legal custody of an individual on parole).

The bill makes a conforming change to the statute that lists the Office of the Inspector General's (OIG) duties by adding the duty to investigate the death of someone in the physical custody of a peace officer, an enforcement agency, or DOC.

Existing law, unchanged by the bill, requires the inspector general to prosecute cases involving unjustifiable use of force by peace officers.

Broadened Authority to Include Federal Officers

The bill expands the above investigatory and prosecutorial authority by applying it to the actions of any federal law enforcement officer. It does this by including a broader definition of "peace officer" within this investigatory statute than what currently applies (see *Background – Peace Officer*).

Under current law, this investigatory authority over federal officers is limited to marshals and deputy marshals and narcotics agents. The bill instead applies it to "federal law enforcement officers," as defined under two federal laws. Specifically, they include any:

1. officer, agent, or employee who the law or a government agency authorizes to prevent, detect, investigate, or prosecute a federal crime (or to supervise these actions) (18 U.S.C. § 115(c)(1)) or
2. employee, including an Amtrak or Federal Reserve law enforcement officer, authorized by law to make arrests or apprehensions and by the employing agency to carry firearms,

who mainly (a) prevents, detects, investigates, prosecutes, or assists in the incarceration of someone who violates the law (or supervises these actions) or (b) protects government officials against personal safety threats (34 U.S.C. § 50301(5)).

Correspondingly, the bill applies this broader definition of “peace officer” to the existing law that sets the standards for determining if use of physical force is justifiable.

Access to Evidence

As part of these use of force investigations, existing law requires the inspector general to ask the appropriate law enforcement agency for any help needed to investigate and determine use of force. The bill specifies that (1) DCJ and the inspector general must have unrestricted access to the scene and to collect evidence as part of these investigations and (2) this right to access applies even if the only peace officers involved in the incident were federal government employees.

The bill allows DCJ or the inspector general to seek injunctive relief in Superior Court against anyone who restricts their access to the scene or to collect evidence.

Under the bill, the court may order declaratory relief (a statement of rights) or a temporary injunction once DCJ’s or the inspector general’s complaint is filed. The court must have a hearing on the complaint within five days after its filing, and the complainant (DCJ or the inspector general) must notify the interested parties of the hearing’s time and location. The court may reschedule the hearing if all parties agree. After the hearing, the court may order, amend, or continue any declaratory relief or temporary injunction.

Subpoena Power

The bill specifies that the inspector general’s authority to issue subpoenas to compel a person’s attendance and testimony in an investigation applies to investigative depositions conducted by the inspector general or his designee.

Reports and Recommendations

Existing law requires the inspector general to file a report with the chief state's attorney after investigating a death from a peace officer's use of force or that happens in a peace officer's or law enforcement agency's custody. The report must include (1) the incident's circumstances; (2) a determination on the use of force (whether it was justifiable), and, currently; (3) recommended future actions for OIG. The bill requires the recommendations to be for the involved law enforcement agency rather than OIG. Relatedly, it allows the inspector general to issue a report on the death of someone in DOC's physical custody, which may include any recommended actions for DOC to take.

Background — Peace Officer

Current law designates the following people as peace officers for purposes of the state's Penal Code and associated statutes: state and local police, DCJ inspectors, state marshals exercising statutory powers, judicial marshals performing their duties, conservation or special conservation officers, constables who have criminal law enforcement duties, appointed special police officers, adult probation officers, DOC officials authorized to make arrests in a correctional institution or facility, investigators in the State Treasurer's Office, certified Department of Motor Vehicles inspectors, U.S. marshals and deputy marshals, U.S. special agents authorized to enforce federal food and drug laws, and certified police officers of a law enforcement unit created and governed under a state-tribal memorandum (CGS § 53a-3(9)).

§ 6 — PROHIBITED FACIAL COVERINGS

Prohibits, subject to several exceptions, peace officers from wearing a facial covering or personal disguise when interacting with the public and performing law enforcement duties; makes a violation a class D misdemeanor

Prohibited Wearing

The bill prohibits, subject to several exceptions, peace officers engaged in law enforcement activities from wearing a facial covering or personal disguise when interacting with the public and performing their duties. Peace officers include federal law enforcement officers, as is the case for use of force investigations under the bill (see §§ 3-5 above).

A violation of the ban on the use of facial covering and personal disguise is a class D misdemeanor, punishable by a fine of up to \$250, up to 30 days in prison, or both. Additionally, an officer who intentionally abuses process or intentionally assaults, batters, falsely imprisons or arrests, or maliciously prosecutes someone (under state or federal law), while knowingly and willfully violating the ban, is unable to use a privilege or immunity defense against a civil liability claim about the officer's actions.

Under the bill, a "facial covering" is an item that conceals or obscures an officer's facial identity, such as opaque masks, garments, helmets, or headgear. Specific examples include balaclavas, tactical masks, gators, and ski masks. "Personal disguise" is undefined.

Exempted Coverings and Uses

The bill allows peace officers to use a medical grade facial covering designed to protect their health and safety, but specifies that this does not include protecting an officer's identity. It also allows them to use facial coverings designed to (1) prevent airborne disease transmission or (2) protect against smoke exposure during a fire. Other exempt facial coverings are those:

1. needed for a water rescue operation,
2. that protect against biological or chemical agent exposure during an incident where there may be an agent,
3. that protect against freezing temperatures during an activity that does not require communicating orally with the public or someone that will be placed in custody, or
4. needed for an active undercover operation or other assignment for which supervising personnel or a court order allow them to be worn.

The bill also allows officers working on a bomb squad, motorcycle unit, or specialized weapons and tactics team to use gear necessary to protect their face and head from physical harm.

§ 6 — BADGE AND NAME TAG IDENTIFICATION

Generally, requires peace officers to be clearly identified by their badge and name tag when making a planned, authorized arrest or interacting with the public in an official capacity; makes an intentional violation a class D misdemeanor

The bill generally requires peace officers (as the bill defines for purposes of use of force investigations, see §§ 3-5 above) to be clearly identified by their badge and name tag. The badge and tag must be (1) on the officer's uniform whenever the officer is authorized to make arrests and is making a planned arrest or interacting with the public in his or her official capacity and (2) worn following existing badge and name tag requirements for police officers.

By law, police officers must already affix and prominently display their badge and name tag on their uniform's outermost garment, unless exempt under the Department of Emergency Services and Public Protection's (DESPP's) model policy on badges and name tags, such as for undercover assignments. The bill similarly exempts a peace officer from the badge and name tag requirement when (1) the officer is working an active undercover assignment; (2) a court order or DESPP's model policy excuses it; or (3) weather-related events or traffic safety issues prevent having the badge or name tag on the outer garment.

An intentional violation of the ban is a class D misdemeanor, which is punishable by a fine of up to \$250, up to 30 days in prison, or both.

§§ 7 & 8 — TAKING INTO CUSTODY IN STATE OR MUNICIPAL FACILITIES OR PROTECTED AREAS

Prohibits peace officers from taking someone into custody on the basis of a civil offense in a state or municipal facility or certain other locations such as schools, hospitals, and houses of worship ("protected areas") without a judicial warrant for the person; applies the definition of "civil offense" to the existing restrictions on taking people into custody on courthouse grounds

The bill prohibits peace officers, from detaining, arresting, or taking someone into custody based on a civil offense in certain locations unless the officer (1) is acting in his or her official capacity and (2) has a judicial warrant for the person. Officers subject to the prohibition are those covered by the bill's expanded definition of "peace officer" for use of force investigations, which includes broader applicability to federal law enforcement (see §§ 3-5 above).

For purposes of these restrictions and the existing ones on taking people into custody on courthouse grounds (see *Background – Detention on Courthouse Grounds*), the bill defines “civil offense” as an offense for which there is a local, state, or federal civil proceeding for the charged person to offer a defense. It does not include an offense that state law identifies as an infraction, a motor vehicle violation, or an arrest that is allowed for any of the following:

1. an alleged criminal violation of (a) a state law or that of any other jurisdiction in the United States that could result in imprisonment as part of the sentence or (b) federal law that could result in imprisonment as part of the sentence and would require an initial appearance before a federal judge, magistrate, or judicial officer;
2. contempt of court, a judge-issued *capias* (warrant), or a warrant for a parole or probation violation; or
3. an emergency commitment or an arrest under the psychiatric disability-related statutes.

The bill allows someone aggrieved by a violation of the ban to bring a civil action in Superior Court, and an action seeking damages is triable by jury. The court may award a plaintiff appropriate legal and equitable relief, such as a temporary or permanent injunction, punitive damages, and attorney’s fees and court costs.

Prohibited Custody Locations

State or Municipal Facilities. State or municipal facilities are buildings owned, leased, occupied, controlled, or used for business by an executive department office or agency or municipal government, and entities that provide direct services on their behalf. This includes the grounds and garages or parking lots that are used as part of the facilities’ operation, regardless of whether they are contiguous (in contact with one another), but not state-owned property leased to a federal entity.

Protected Areas. The bill’s protection from being taken into custody in certain areas applies to the following buildings or locations, including

their grounds and garages or parking lots that are used as part of their operation, regardless of whether they are contiguous:

1. schools, ranging from preschools to colleges or universities;
2. licensed hospitals or urgent care centers;
3. places of worship or religious study;
4. social services establishments, such as crisis centers, shelters, supervised visitation or family justice centers, victim services centers, food banks or pantries, or substance counseling and treatment facilities;
5. places for disaster or emergency response and relief, including supply distribution sites, to register for disaster-related assistance, or to be reunited with family;
6. cemeteries or other internment locations; and
7. playgrounds, recreation or child care centers, before- or after-school care centers, foster care facilities, group homes for children, or school bus stops when children are there.

Background — Detention on Courthouse Grounds

Under existing law, to take a person into custody on courthouse grounds based on a civil offense, a state, local, or federal law enforcement representative must (1) be operating in his or her official capacity and (2) have first notified a judicial marshal in the courthouse. The representative must also give the marshal documentation showing that the person to be detained, arrested, or taken into custody is (1) the subject of a judicial warrant or (2) exempt from the protections of the state’s civil detainer law (because of a specified criminal conviction or possible match in a terrorist database) (CGS § 51-33b).

§ 9 — POST CERTIFICATION OF POLICE OFFICERS

Prohibits POST from waiving the basic training program requirements to be certified as a police officer for peace officers unless they give evidence of satisfactorily completing a substantially equivalent training or education program with at least 480 training hours

Existing law generally prohibits someone from being employed as a police officer by a law enforcement unit for more than one year without being certified by POST. POST's certification process requires completing a basic training program. But POST may certify applicants who (1) show that they satisfactorily completed an equivalent program or course in another state or as part of armed forces training and (2) pass a test or evaluation. Related, current regulations allow POST to waive all or parts of the basic training requirement for these applicants under certain circumstances (Conn. Agencies Reg. § 7-294e-2).

The bill prohibits POST from waiving any part of its required basic training program for an applicant who served or is serving as a peace officer (as defined by the bill for use of force investigations, see §§ 3-5 above) unless the applicant gives evidence of satisfactorily completing a substantially equivalent training or education program with at least 480 training hours. But the bill further specifies that POST is not required to waive any part of the basic training program for these peace officers.

§ 10 — OFFICER INTERFERENCE WITH PHOTO OR VIDEO TAKING

Makes federal law enforcement agencies liable when their officers interfere with someone taking a photo, digital still, or video image of them or another officer performing their duties; makes an immunity defense unavailable in a civil liability action for an intentional tort committed while interfering with the taking of the photo, digital still, or video image

Current law makes a peace officer's employer liable if the officer interferes with someone taking a photo or digital still or video image of the officer or another officer performing his or her duties, subject to several exceptions. But it exempts federal government special agents and specified tribes' law enforcement unit members.

The bill generally applies its expanded definition of peace officer for inspector general use of force investigations (see §§ 3-5 above) to this provision, making the liability apply to the employers of all federal law enforcement officers, but keeping the exemption for tribal law

enforcement.

Existing law exempts an employer from liability under certain specified circumstances, including when the officer had reasonable grounds to believe that the interference was to lawfully enforce a state criminal law or municipal ordinance. The bill, conforming with its liability expansion to federal agencies, broadens the exemption to include lawful enforcement of a federal criminal law.

Additionally, if a peace officer intentionally abuses process or intentionally assaults, batters, falsely imprisons or arrests, or maliciously prosecutes (either under state or federal law) someone while interfering with someone taking a photo, digital still, or video of him- or herself or another officer, the officer is unable to use a privilege or immunity defense against a civil tort liability claim about the actions.

§ 11 — PROSECUTORIAL IMMUNITY FOR FEDERAL ACTIONS

Limits the circumstances under which a federal officer, employee, or agent has immunity when prosecuted for an offense based on an action taken under color of law

The bill limits circumstances under which a federal officer, employee, or agent has immunity when prosecuted for an offense based on an action taken under color of law (the appearance of authority from federal law). Specifically, the immunity applies when the action was authorized by federal law and was necessary and proper to execute official duties.

§ 12 — POLICE OFFICER HIRING PROHIBITION

Extends to all peace officers the current prohibition on hiring police officers who (1) were dismissed for malfeasance or serious misconduct or (2) resigned or retired during an investigation for this conduct

The bill broadens the prohibition on a law enforcement unit (generally state or local police) from hiring a police officer who was previously employed by the unit or in another jurisdiction and (1) was dismissed for malfeasance or serious misconduct calling into question their fitness to serve as an officer or (2) resigned or retired during an investigation for this conduct.

It does this by replacing the term “police officer” with “peace officer”

and in doing so applies the hiring prohibition to hiring peace officers. Under the bill, as is the case for the inspector general's expanded investigative authority, peace officers include all federal law enforcement officers and other state employees like state or judicial marshals and certain correctional employees (see §§ 3-5 above). Currently, the prohibition covers hiring sworn members of organized local police departments, appointed constables with criminal law enforcement duties, special policemen appointed for state property or utility or transportation companies or to investigate public assistance fraud, and any member of a law enforcement unit who performs police duties.

As under existing law, the hiring prohibition does not apply to an officer exonerated of all malfeasance or serious misconduct allegations.

For purposes of the law and the bill, (1) "malfeasance" has its common meaning (wrongdoing), and (2) "serious misconduct" is an officer's improper or illegal actions connected with official duties that could cause a miscarriage of justice or discrimination, such as a felony conviction, evidence fabrication, repeated use of excessive force, bribe acceptance, or fraud.

§§ 13-15 — AUTOMATED LICENSE PLATE READER SYSTEMS

Sets various conditions and restrictions on how law enforcement agencies and other public agencies may use ALPR systems or associated data, including limits on (1) when they can use these systems or data or share the data and (2) how long they can keep the data; sets related requirements and restrictions for private vendors contracting with public agencies for these purposes; allows the attorney general (as to vendors) or private parties to seek related court relief and POST to discipline law enforcement officers for certain malicious conduct; requires POST to adopt a model ALPR usage policy and DESPP to adopt related regulations for implementation by law enforcement agencies; requires POST, in consultation with UConn's Institute for Municipal and Regional Policy, to develop a standardized form for reporting ALPR system usage and sets related reporting requirements

Starting October 1, 2026, this bill restricts law enforcement agencies (such as municipal police departments or the State Police), other public agencies, and private vendors under contract with them from using automated license plate reader (ALPR) systems or ALPR data, except for certain listed reasons. Among other things, it:

1. sets a 21-day limit on how long agencies can keep this data unless certain conditions are met (such as its use in an active criminal investigation);
2. specifically prohibits several uses of ALPR systems or data, such as for investigating suspected immigration violations;
3. establishes requirements and restrictions for ALPR contracts between agencies and private vendors;
4. allows the attorney general or private parties to go to court to enforce specified violations and POST to take disciplinary action against law enforcement officers for certain malicious conduct;
5. requires POST to adopt a model ALPR usage policy and DESPP to adopt related regulations for implementation by law enforcement agencies;
6. requires POST, in consultation with UConn's Institute for Municipal and Regional Policy (IMRP), to develop a standardized form for reporting ALPR system usage; and
7. sets related reporting requirements for law enforcement agencies, other public agencies, and UConn's IMRP.

Under the bill, an "ALPR system" is a mobile or fixed electronic image recording device that, in combination with computer programs or algorithms, can convert images of license plates or vehicle descriptors into computer-readable data. But it does not include an image recording device that provides evidence used to enforce an offense specified in a state statute or municipal ordinance, including an automated traffic enforcement safety device (speed or red light camera), or those used as part of a work zone speed control system or a municipal school bus violation enforcement system.

"ALPR data" is any data that an ALPR system captures, records, holds, or stores, or processes, or that is derived from the system. This includes license plate characters, vehicles' still or video images, vehicle attributes, location data, time stamps, and metadata.

Permissible Uses (§ 13(b))

Starting on October 1, 2026, the bill prohibits public agencies (see *Background – Public Agencies*), or private vendors under contract with them, from operating ALPR systems or using ALPR data, except under the following conditions.

Public Agency or Vendor Uses. Under the bill, public agencies or private vendors under contract with them may operate these systems or use this data to:

1. perform weigh station duties;
2. monitor or maintain their own vehicles or equipment;
3. help in controlling access to secured areas;
4. analyze traffic;
5. enforce parking regulations and collect associated fines, including (a) by a municipal parking authority or (b) on the grounds of a facility owned or operated by any other public agency and any garages or parking lots the facilities use (next to the facility or otherwise);
6. enforce motor vehicle property tax compliance; and
7. monitor and secure state facilities.

Under the bill, a “state facility” is any building (or part of one) owned, leased, occupied, controlled by, or used for business by an office or agency of the state executive, legislative, or judicial branch. This includes entities providing direct services on their behalf, but not state-owned property leased to a federal entity. It also includes the grounds of these facilities and any garages or parking lots they use (next to the facility or otherwise).

Law Enforcement or Vendor Uses. The bill allows law enforcement agencies or private vendors under contract with them to operate these systems or use this data to compare with data in:

1. a hotlist (a list of registration numbers on license plates, kept for purposes of this comparison) or internal hotlist addendum (see below);
2. the Connecticut Online Law Enforcement Communications Teleprocessing (COLLECT) system;
3. the FBI's Kidnapping and Missing Persons list;
4. the Connecticut Criminal Justice Information System;
5. the federal Terrorist Screening Database;
6. the National Crime Information Center (NCIC) database; or
7. the National Center for Missing and Exploited Children database.

Under the bill, an "internal hotlist addendum" is a hotlist that (1) is kept for use only at a specific state facility or facilities for which the list was made and by the public agency that made it, and (2) may contain registration numbers displayed on a vehicle license plate registered to a person identified as a potential threat to someone in the facility, the facility itself, or the agency operating it. These threats may be shown by the person's previous conviction for an offense involving threats of violence or harassment, or documented conduct involving threatened or attempted violence, harassment, or incitement to violence, against someone in the facility, the facility itself, or the agency. But an internal hotlist addendum item cannot be based on an arrest for, or conduct that is, solely constitutionally protected speech, conduct, or association (under the First Amendment or the state constitution's Article First).

The bill also allows law enforcement agencies and their private vendors to enter license plate numbers into an ALPR system if an officer determined that system data may:

1. help to apprehend someone with an outstanding warrant,
2. help to locate a missing or endangered person or to recover a

stolen vehicle, or

3. be relevant and material to a specific active criminal investigation.

For criminal investigations, this use is allowed only if there is a reasonable suspicion that the offense has been or is being committed. The agency must keep a record of (1) the reason for accessing the data and (2) any associated case number for the complaint or incident.

Retention Limit. The bill generally allows public agencies or private vendors under contract with them to keep ALPR data (regardless of how it was acquired) for only 21 days. But they must keep it for a shorter period if that is required by a contract between the agency and a private vendor that accesses the system or holds or stores the data.

These periods do not apply to data being kept:

1. under a state or federal judicial warrant or court order;
2. under court rules on preserving evidence;
3. for collecting highway usage fees (if they exist), but the data must be deleted within 30 days after the fee is collected;
4. for analyzing traffic, if the data is held, stored, or managed as de-identified, aggregated, or summarized data; or
5. as evidence in an active criminal investigation or prosecution.

For this last reason, a supervisory law enforcement officer must approve the longer retention period, and the agency must keep a record of (1) the purpose for keeping the data and (2) any associated case number. Unless a warrant, court order, or rules of evidence require otherwise, the data must be deleted upon (1) the investigation's conclusion, if no charges are filed; (2) if there is a conviction without a prison sentence, the case's final disposition, including all direct appeals being exhausted; or (3) if there is a conviction with a prison sentence, the release of the last person imprisoned for a conviction to which the

data relates.

The bill also allows public agencies or their private vendors to keep ALPR data for more than 21 days if it may be necessary to establish that a potential future offense, motor vehicle violation, or infraction (under an ordinance, statute, or regulation) is a subsequent one with a higher penalty than the previous one.

Additionally, if ALPR data is collected for purposes of enforcing motor vehicle property tax compliance, it may be kept for longer than 21 days if the data is (1) kept expressly for that purpose, (2) not shared with anyone other than the municipality's tax assessor or the individual to whom the vehicle is registered, and (3) deleted after 90 days or following the tax assessor's determination of compliance, whichever occurs first.

Use as Evidence (§ 13(c))

The bill allows ALPR data to be admissible as evidence in Connecticut courts, as long as the data was collected or otherwise acquired, held, or stored in line with the bill or obtained under a warrant issued by a Superior Court judge.

Specifically Prohibited Uses and Exceptions (§ 13(d) & (l))

The bill prohibits public agencies from operating an ALPR system or using ALPR data for various purposes. These prohibitions apply starting on October 1, 2026.

Various Prohibitions. Specifically, it bars them from using or helping in the use of ALPR data to monitor or investigate someone based on their actual or perceived race, ethnicity, sexual orientation, gender identity or expression, sex, pregnancy status, disability, citizenship, nationality, or income, or their perceived criminal history (except when someone is being investigated for a potential crime for which an element of the offense is a prior conviction).

It also bars them from using or helping in the use of an ALPR system or ALPR data to:

1. identify someone engaged in an activity protected by the First Amendment;
2. investigate a suspected immigration violation or otherwise help in civil or criminal immigration enforcement; or
3. investigate or prosecute someone who has sought, received, or provided reproductive or gender-affirming health care services that are legal under state law.

Collection Near Gender-Affirming Care Facilities or Facilities Serving Immigrants. The bill also generally bars public agencies from collecting ALPR data from a fixed ALPR system at or near a (1) reproductive or sexual health facility that primarily provides gender-affirming health care services that are legal under state law or (2) nonprofit or community organization that primarily serves immigrant communities. It requires POST to establish a distance for this prohibition (see below).

For these prohibitions to apply, the facility or organization must notify POST of its location. The prohibitions do not apply (1) if collecting the data would be allowed under the law on police body and dashboard cameras or (2) to properties under federal jurisdiction.

Information Sharing. The bill also restricts when these agencies can share or provide access to ALPR data. It allows them to do so only if the requesting person or entity is:

1. an individual requesting data for a vehicle registered in his or her own name (if a vehicle has multiple owners, lessors, or regular users, they all must be individuals and must join in the request);
2. another Connecticut public agency; or
3. under certain conditions, a law enforcement agency from another jurisdiction or multi-jurisdictional task force.

Under the bill, public agencies can share ALPR data with a state or municipal law enforcement agency from Massachusetts, New York, or

Rhode Island, or a multi-jurisdictional task force of which the Connecticut agency is a member, but only if the requesting agency or task force affirms in writing that in using the data, it will comply with the bill's prohibitions and will not:

1. use it for immigration investigations or enforcement,
2. use it for investigations or prosecutions relating to reproductive or gender-affirming health care services that are legal under Connecticut law, or
3. further disclose it except as allowed by Connecticut law.

Additionally, for a task force, the group's head or designee must have approved the specific data request, and the data must be directly and reasonably relevant to a specific investigation.

The bill also allows Connecticut agencies to share data with other law enforcement agencies (including federal ones), but only if the requesting agency has a judicially issued probable cause warrant for the specific data requested or is requesting specific data on a possible match in the federal Terrorist Screening Database.

Under the bill, a Connecticut law enforcement agency must notify POST if, after sharing ALPR data with another state's or a federal law enforcement agency, the Connecticut agency suspects that the other agency may have used the data in a way prohibited by the bill. POST must determine whether this occurred and, if so, direct each Connecticut law enforcement agency to discontinue sharing ALPR data with, or giving ALPR data access to, the other agency.

Network Participation. Unless certain conditions are met, the bill bars public agencies from (1) participating in a system or network that shares ALPR data or (2) giving data to or accessing it through a multi-state, intrastate, or national data-sharing system or network. This is allowed only if the system or network requires participants to execute a written declaration affirming that the shared, accessed, or otherwise acquired data will be used solely in line with the bill and other

Connecticut law and that they will not share or use the data except in line with the bill.

Bulk or Automatic Access. The bill also bars these agencies from allowing a public agency to have real-time, bulk, or automatic access to ALPR data, unless (1) it is in response to a documented, case-specific request and (2) the bill does not otherwise prohibit the data sharing.

Limits on Data Disclosure Under FOIA and Exceptions (§ 13(e))

The bill makes ALPR data confidential and prohibits it from being deemed a public record under the Freedom of Information Act (FOIA). But it deems the following as public records, making them generally disclosable under FOIA:

1. the locations of ALPR recording devices (of video or still images), unless the device's purchase was funded in whole or part by the U.S. Department of Homeland Security and the funding was conditioned on the device's location being kept confidential and
2. data derived from an ALPR system audit, system usage logs, and data access logs, as long as ALPR data is redacted.

The bill allows people to get, from the contracting public agency, ALPR data about vehicles that are registered in their name (if the vehicle is also registered in someone else's name, that person also must consent to the disclosure).

Required Policies for Non-Police Public Agencies (§ 13(f))

The bill requires public agencies (other than law enforcement agencies) that operate ALPR systems or use ALPR data to adopt and make public a written usage and privacy policy. They must do this by January 1, 2027, and before they use or acquire a system or data. The policy must (1) comply with the bill's applicable provisions and (2) include standards and safeguards substantially equivalent to those required under POST's model policy (see below).

Contracts With Private Vendors; Attorney General Enforcement (§ 13(g)-(i))

The bill prohibits public agencies from entering or renewing contracts with private vendors related to ALPR system usage or data unless the contract bars the vendor from engaging in certain activities with respect to ALPR data collected in the state. This applies despite any contrary terms of service (such as conditions of use or vendor policies) that are incorporated by reference or otherwise part of the contract.

The contract must bar the vendor from:

1. selling the ALPR data;
2. sharing or transferring it with or to any third party without the contracting agency's express written authorization to share or transfer it for a specific purpose;
3. allowing anyone other than the contracting agency to access the ALPR data, unless the vendor must allow this due to a Connecticut or federal warrant or court order (but not a subpoena or demand of a grand jury investigation); or
4. holding or storing the contracting agency's ALPR data (a) with ALPR data it holds or stores under a contract with a different agency or other person or (b) in a way that does not align with industry-recognized data security practices, such as using encryption when sending or storing it.

The contract also must bar the vendor from sharing or transferring ALPR data, or allowing access to it, if the vendor reasonably believes that the data will be used for:

1. investigating a suspected immigration violation or otherwise helping in immigration enforcement;
2. investigating or prosecuting anyone for allegedly (a) seeking, providing, or receiving reproductive or gender-affirming health care services that are legal under Connecticut law or (b) helping someone else to do so (for example, by giving information,

transportation, lodging, or material support for these activities);
or

3. any effort to identify or impose civil or criminal liability on someone solely for an activity that is protected by the state or federal constitution, including someone exercising the right to free speech, peaceable assembly, or petition the government for a redress of grievances, except as otherwise provided by state or federal law.

The bill also prohibits public agencies from entering into or renewing ALPR-related contracts with private vendors unless the contract requires (1) the vendor to consent to personal jurisdiction in Connecticut in the event of a legal proceeding and (2) Connecticut law to govern the contract.

Under the bill, if a private vendor under contract with a public agency engages in any of the prohibited conduct described above with respect to ALPR data collected in the state, the attorney general may bring an action against the vendor. In these cases, the court may grant appropriate relief, including injunctive or declaratory relief, damages, and any other available relief under law. If the attorney general prevails, the court must order that any awarded damages are given to the injured person. The court may also award civil penalties against each defendant, up to \$2,500 per violation, to be deposited in the General Fund.

Private Enforcement (§ 13(j))

Starting October 1, 2026, the bill allows an aggrieved individual to bring an action against a public agency for injunctive or declaratory relief, including a determination of past violations. This applies if the agency's officer, employee, or agent violates any of the bill's provisions on permissible or prohibited uses or data sharing (including under FOIA). If a private vendor committed the violation, or the vendor engaged in any of the conduct prohibited under these contracts (see above) with respect to ALPR data collected in the state, the vendor itself (and not the agency) is liable.

Under the bill, an aggrieved individual can bring the case in the judicial district where he or she lives. If the individual prevails and is granted an order for injunctive relief, the individual may be entitled to recover court costs and reasonable attorney's fees (but only with respect to the case, or part of it, related to seeking and getting the injunction).

These cases must be privileged (prioritized) with respect to trial assignment.

POST Disciplinary Action (§ 13(k))

Under the bill, if a law enforcement officer is found to have knowingly accessed, used, or distributed ALPR data with malicious intent for purposes outside of the bill's allowable uses, the officer is subject to disciplinary action including suspension, cancellation, or revocation of his or her POST certification.

POST Policy and Law Enforcement Adoption (§ 14(a) & (b))

By December 1, 2026, the bill requires POST to adopt a model policy on law enforcement agencies' acquisition and use of ALPR systems and data. The policy must direct these agencies to comply with the bill's ALPR provisions, including allowed and prohibited uses of ALPR systems and data (whether collected by the ALPR system or acquired otherwise). The policy must also:

1. set standards for using a hotlist (including permissible sources) and supervisory approval requirements for using hotlist data, and managing, accessing, and validating the data (including time limits to include data on a hotlist);
2. set data retention limits in line with the bill's requirements (see above);
3. set data access and sharing requirements in line with the bill, including internal access controls and supervisory review and conditions under which the data may be shared with other public agencies or law enforcement agencies;
4. provide for a supervisory responsibility and accountability

- structure, including designating an officer or unit responsible for overseeing ALPR system use and complying with the policy;
5. set training requirements, including for officers and employees authorized to access the system or data;
 6. set audit and logging requirements, including for access logs (see below), with audits done at least quarterly;
 7. set public transparency standards and requirements, including for publication of agency-specific ALPR system usage policies and annual statistical reports on this usage;
 8. set the distance for the general prohibition on collecting ALPR data near (a) facilities that primarily provide gender-affirming health care or (b) nonprofits or organizations that primarily serve immigrant communities (see above); and
 9. include provisions on compliance with the bill's private vendor-related provisions (see above).

The model policy's provisions on access logs must ensure compliance and facilitate independent review. The logs must document the access and retention of ALPR data, including how often the data is kept and for how long.

The bill requires each law enforcement agency, by January 1, 2027, to adopt and implement either POST's model policy or another policy that gives greater privacy protections than the model policy. Law enforcement agency policies are in effect until DESPP's regulations are adopted (see below). Once adopted, the regulations supersede agency policies.

DESPP Regulations (§ 14(c))

By January 1, 2028, the bill requires the DESPP commissioner, in consultation with POST, to adopt regulations setting a policy in line with the requirements for POST's model policy and the bill's other ALPR provisions. By January 1, 2033, and at least every five years after,

the commissioner, in consultation with POST, must update the regulations based on any changes in law, technology, or best practices. The updated regulations must not reduce or limit the bill's protections or minimum standards.

These regulations are binding on all law enforcement agencies.

Standardized Form (§ 15(a))

The bill requires POST, by January 1, 2027, and in consultation with DESPP and UConn's Institute for Municipal and Regional Policy (IMRP), to develop a standardized form for reporting ALPR system usage. The form must include the number of:

1. license plates scanned;
2. searches done by the law enforcement agency due to ALPR system use and the reasons why;
3. times ALPR data was shared with or accessed by other entities, their identities, and the reasons why;
4. times ALPR data was shared or accessed under a judicial warrant;
5. any instances when the data was kept longer than allowed under the bill;
6. any instances when the data was requested to be collected at (a) facilities that primarily provide gender-affirming health care or (b) nonprofits or organizations that primarily serve immigrant communities; and
7. times the data was accessed or requested on the 14th day or later after it was collected.

The form also must include any changes to the law enforcement agency's data collection, retention, or sharing policies that affect ALPR data privacy.

ALPR Usage Reporting (§ 15(b) & (c))

Under the bill, if a law enforcement agency uses an ALPR system, it must annually report to UConn’s IMRP, using the standard form, and publish the report on the agency’s website. If another public agency uses an ALPR system, it must post an annual report on its website about that usage, with the applicable information from the standard reporting form.

In either case, the reporting or posting is due by January 31 following any year when the agency uses an ALPR system.

IMRP Reporting (§ 15(d))

The bill requires UConn’s IMRP to annually compile, analyze, and summarize the submitted reports and prepare a consolidated report on ALPR usage along with any legislative recommendations. The report must be sent to the governor and the Judiciary and Public Safety and Security committees, with the first report due by July 30, 2027.

Background — Public Agencies

Under FOIA and the bill, a public agency generally includes any:

1. executive, administrative, or legislative office of the state or any political subdivision of the state and any state or town agency;
2. department, board, commission, authority, or official of the state or of any municipality, school district, or other district or other political subdivision;
3. committee of, or created by, any of these offices or officials;
4. judicial office, official, or body or committee, but only for administrative functions; and
5. person to the extent they are the functional equivalent of a public agency (CGS § 1-200(1)).

BACKGROUND — RELATED BILLS***ALPR Provisions***

sSB 4 (File 285), § 18, favorably reported by the General Law Committee, prohibits the departments of transportation and motor vehicles, and law enforcement agencies, from contracting with ALPR users unless the contract bars the user from taking various actions.

sHB 5449 (File 536), favorably reported by the Judiciary Committee, restricts public agencies or law enforcement agencies from using ALPR systems, or using or sharing ALPR data, except for listed reasons, and requires related policies and reporting.

sHB 5552 (File 555), favorably reported by the Government Administration and Elections Committee, prohibits public agencies from contracting with ALPR vendors unless the contract bars the vendor from taking various actions.

Inspector General Investigations; Custody Actions for Civil Offenses

sSB 91 (File 491), favorably reported by the Judiciary Committee, also (1) gives the inspector general the investigatory authority over physical force incidents involving federal law enforcement officers and (2) restricts taking people into custody based on a civil offense in state or municipal facilities and protected areas.

sHB 5428 (File 599), favorably reported by the Judiciary Committee, also (1) limits the inspector general's investigations of custody deaths to those that occur in a peace officer's, law enforcement agency's, or DOC's physical custody; (2) revises the inspector general's reporting authority after investigations; and (3) specifies that the inspector general's authority to issue subpoenas applies to investigative depositions.

Election Site Custody Prohibition; Attorney General Civil Rights Actions

sSB 463 (File 570), §§ 1 & 8, and sHB 5533 (File 548), §§ 1 & 8, favorably reported by the Government Administration and Elections Committee, among other things, (1) generally prohibit state and federal officers and agents from searching, detaining, or arresting people within

250 feet of an election site and (2) expand the state attorney general's authority to investigate and bring actions for certain civil rights violations, under state or federal law or constitutions, to include when a person has a policy that violates them.

COMMITTEE ACTION

Judiciary Committee

Joint Favorable Substitute

Yea 30 Nay 11 (03/23/2026)